UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/714,520	11/17/2003	Lionel Belnet	550-482	6838

23117 7590 12/05/2005

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
FLOURNOY, HORACE L	
ART UNIT	**PAPER NUMBER**
2189	

DATE MAILED: 12/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/714,520	BELNET ET AL.	
	Examiner	Art Unit	
	Horace L. Flournoy	2189	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 November 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 November 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

The instant application having Application No. **10/714,520** has a total of *20* claims pending in the application; there are *4* independent claims and *16* dependent claims, all of which are ready for examination by the examiner.

INFORMATION CONCERNING OATH/DECLARATION

Oath/Declaration

The applicant's oath/declaration has been reviewed by the examiner and is found to conform to the requirements prescribed in **37 C.F.R. 1.63**.

STATUS OF CLAIM FOR PRIORITY IN THE APPLICATION

As required by **M.P.E.P. 201.14(c),** acknowledgement is made of applicant's claim for priority based on an application filed on November 18, 2002 (Foreign Priority 0226882.9).

ACKNOWLEDGEMENT OF REFERENCES CITED BY APPLICANT

As required by **M.P.E.P.** 609(c), the applicant's submission of the Information Disclosure Statements dated **04/20/2004** and **11/17/2005** are acknowledged by the examiner and the cited references have been considered in the examination of the

claims now pending. As required by **M.P.E.P.** 609(c), a copy of the PTOL-1449 initialed and dated by the examiner is attached to the instant office action.

REJECTIONS NOT BASED ON PRIOR ART

Double Patenting

Copending applications 10/714,520 (instant) and 10/714,481 were found to have obviousness-type provisional double-patenting issues. 10/714,520 was found to have broader claims than the instant application.

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., In re Berg, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); In re Goodman, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); In re Longi, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); In re Van Ornum, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); In re Vogel, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and In re Thorington, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1, 2, 5, 8-11, 14, 17, 18, and 20 are provisionally rejected under the judicially created doctrine of nonstatutory obviousness-type double patenting as being

unpatentable over claims 1, 3, 4, and 9 of copending Application No. 10/714,481. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1, 2, 5, 8-11, 14, 17, 18, and 20 of the instant application and claims 1, 3, 4, and 9 of copending Application No. 10/714,481 each claim similar if not identical limitations. All of this is explained below in detail.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

With respect to claims 1, 10, and 20 of the instant application, please refer to the table below, which illustrates the anticipatory relationship of the claims at issue:

Instant Application 10/714,520		**Copending Application 10/714,481**	
Claim No.	**Limitation**	**Claim No.**	**Limitation**
1	A data processing apparatus	3	A data processing apparatus, *comprising: a processor operable in a plurality of modes and a*

	having a secure domain and a non-secure domain,		plurality of domains, said plurality of domains comprising a secure domain and a non-secure domain, *said plurality of modes including at least one non-secure mode being a mode in the non-secure domain and at least one secure mode being a mode in the secure domain*,
	in the secure domain the data processing apparatus having access to secure data which is not accessible in the non-secure domain,		*said processor being operable such that when executing a program in a secure mode said program* has access to secure data which is not accessible when said processor is operating in a non-secure mode

	the data processing apparatus comprising: a device bus;		*A data processing apparatus as claimed in claim 1, wherein the memory unit is coupled to the processor via* a processor bus, the memory unit and processor forming a device, and the data processing apparatus further comprises a device bus *via which the device is connectable to a further memory unit, the further memory unit having secure memory for storing secure data and non-secure memory for storing non-secure data.*

	a device coupled to the device bus and operable to issue a memory access request pertaining to either said secure domain or said non-secure domain;		the memory unit and processor forming a device, and the data processing apparatus further comprises a device bus *via which the device is connectable to a further memory unit, the further memory unit having secure memory for storing secure data and non-secure memory for storing non-secure data....when the processor is operating in said at least one non-secure mode, the memory unit being operable,* upon receipt of a memory access request issued by the processor when access to an item of data is required, to prevent access to any data item within an entry of the memory unit that the associated flag indicates has secure data stored therein.

	and a memory coupled to the device bus and operable to store data required by the device,		a memory *unit comprising a plurality of entries* and operable to store data required by the processor
	the memory comprising secure memory for storing secure data and non-secure memory for storing non-secure data;		*A data processing apparatus as claimed in claim 1, wherein the memory unit is coupled to the processor via a processor bus, the memory unit and processor forming a device, and the data processing apparatus further comprises a device bus via which the device is connectable to a further memory unit, the further* memory unit having secure memory for storing secure data and non-secure memory for storing non-secure data.

	the device being operable to issue onto the device bus the memory access request when access to an item of data in the memory is required,		*when the processor is operating in said at least one non-secure mode, the memory unit being operable,* upon receipt of a memory access request issued by the processor when access to an item of data is required, *to prevent access to any data item within an entry of the memory unit that the associated flag indicates has secure data stored therein.*
	the memory access request issued by the device including a domain signal identifying whether the memory access request pertains to said secure domain or said non-secure domain.		*each entry being operable to store one or more data items consisting of either secure data or non-secure data,* and a flag being associated with each entry in the memory unit to store a value indicating whether the one or more data items stored in the associated entry are said secure data or said non-secure data;

With respect to claims 2 and 11 of the instant application, the limitations are taught in the copending Application No. 10/714,481 in **claim 1**.

With respect to claims 5 and 14 of the instant application, the limitations are taught in the copending Application No. 10/714,481 in **claim 4**.

With respect to claims 8 and 17 of the instant application, the limitations are taught in the copending Application No. 10/714,481 in **claim 9**.

With respect to claims 9 and 18 of the instant application, the limitations are taught in the copending Application No. 10/714,481 in **claim 4**.

REJECTIONS BASED ON PRIOR ART

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-20 are rejected under 35 U.S.C. 102(e) as being anticipated by **Gardner et al. (U.S. PG PUB No. 2003/0101322 hereafter referred to as Gardner).**

With respect to independent **claims 1, 10, 19 and 20**,

(Note: the examiner interprets independent claims 1, 10, 19, and 20 in the same way because of identical or patentably indistinct limitations)

"A data processing apparatus **[Gardner discloses in paragraph [0002], "Computer systems include at least one processor and memory." See FIG. 3]** *having a secure domain and a non-secure domain* **[Gardner discloses in paragraph [0189], "secure and non-secure"]**, *in the secure domain the data processing apparatus having access to secure data which is not accessible in the non-secure domain* **[Gardner discloses in paragraph [0026], "Secure platform 40, however, ensures that one domain cannot accidentally or intentionally access another domain's memory."]**,"

"...the data processing apparatus comprising: a device bus; **[Gardner discloses in FIG. 3, the memory unit (element 20) coupled to the processor (element 32) via a device bus (connection between). With respect to this limitation Gardner also discloses the Intel IA-64 architecture which utilizes device bus(es).]"**

"...a device coupled to the device bus and operable to issue a memory access request pertaining to either said secure domain or said non-secure domain **[As per this limitation, it is notoriously well known that the Intel Architecture (IA-64) and the HP Precision Architecture (PA-RISC) comprises a device bus which is operable to issue a memory access request. Gardner teaches**

in paragraph [0026], that the memory access request can pertain to either a secure domain or a non-secure domain];"

"...and a memory coupled to the device bus **[FIG. 3, element 20]** *and operable to store data required by the device, the memory comprising secure memory for storing secure data and non-secure memory for storing non-secure data* **[paragraph [0189]];"**

"... the device being operable to issue onto the device bus the memory access request **[paragraph [0026], "access...memory"]** *when access to an item of data in the memory is required, the memory access request issued by the device including a domain signal identifying whether the memory access request pertains to said secure domain or said non-secure domain* **[Gardner discloses in paragraph [0189], "...secure user processes are distinguished from non-secure user processes by setting a bit in the "magic number" or ELF (Executable and Linkable Format) header...the information for distinguishing between secure and non-secure user processes is contained in a secure memory page in memory 74."].**"

With respect to **claims 2, 11 and 19**,

"A data processing apparatus as claimed in claim 1 **[see rejection of claim 1]**, *wherein the device is operable in a plurality of modes* **[Gardner discloses in paragraph [0189], "user processes" (see also execution privilege levels)]**, *including at least one non-secure mode being a mode in the non-secure domain* **["secure and non-secure user processes"]** *and at least one secure mode*

being a mode in the secure domain **Gardner discloses in paragraph [0062], "...when processor 32 is implemented as an IA-64 processor, processor privilege level, region IDs, protection keys, and page access rights are primitives upon which domains and processes are protected from one another in SPA 30"].**"

With respect to **claims 3 and 12**,

"A data processing apparatus as claimed in claim 1 **[see rejection of claim 1]**, *wherein the device has a predetermined pin for outputting the domain signal onto the device bus* **[Gardner discloses in paragraph [0189], "...secure user processes are distinguished from non-secure user processes by setting a bit in the "magic number" or ELF (Executable and Linkable Format) header...the information for distinguishing between secure and non-secure user processes is contained in a secure memory page in memory 74."].**"

With respect to **claims 4 and 13**,

"A data processing apparatus as claimed in claim 1 **[see rejection of claim 1]**, *wherein in said non-secure domain the device is operable under the control of a non-secure operating system,* **[Gardner discloses in paragraph [0004], "...user applications employ a non-privileged instruction set provided by the processor hardware and an application program interface (API) defined by the operating system." Gardner also teaches in paragraph [0188], that in**

a non-secure domain the device is operable under the control of a non-secure operating system: "...non-secure application (running at PL3), such as an end user application 44."]"

"...and in said secure domain the device is operable under the control of a secure operating system[**Gardner discloses in paragraph [0033], "End user applications 44 run at the least privileged level, PL3, as unprivileged tasks under the control of an operating system image 42 in a secure platform 40 protection domain."**]*."*

With respect to **claims 5 and 14**,

"A data processing apparatus as claimed in claim 1[**see rejection of claim 1**]*, further comprising partition checking logic coupled to the device bus* [**SPK of FIG. 3, element 36**] *and operable whenever the memory access request as issued by the device pertains to said non-secure domain to detect if the memory access request is seeking to access the secure memory, and upon such detection to prevent the access specified by that memory access request* [**Gardner discloses in paragraph [0026], "Secure platform 40, however, ensures that one domain cannot accidentally or intentionally access another domain's memory."**] *."* (Also see **paragraphs [0195] and [0146]**).

With respect to **claims 6 and 15**,

"A data processing apparatus as claimed in claim 5 **[see rejection of claim 5]**, *wherein the partition checking logic is managed by the device when operating in a predetermined secure mode in said secure domain* **[Gardner discloses in paragraph [0195], "Using the memory management services of SPK 36, a user application is able to create secure memory partitions and processes..."]**."

With respect to **claims 7 and 16**,

"A data processing apparatus as claimed in claim 5 **[see rejection of claim 5]**, *wherein the partition checking logic is provided within an arbiter coupled to the device bus* **[SPK of FIG. 3, element 36]** *to arbitrate between memory access requests* **[paragraphs [0133]-[0135]]** *issued on the device bus* **[stated supra in rejection of claim 1]**."

With respect to **claims 8 and 17**,

"A data processing apparatus as claimed in claim 1 **[see rejection of claim 1]**, *wherein the device is a chip incorporating a processor* **[paragraph [0003]]**,"

"...the chip further comprising a memory management unit... **[Gardner discloses in paragraph [0022], "SPK 36 is preferably a small kernel of trusted, provably correct code that performs all security critical services. Example security critical services include memory and process management..."]"** **(FIG. 3)**

"...operable, when the processor generates the memory access request **[see rejection of claim 1]**, *to perform one or more predetermined access control functions to control issuance of the memory access request onto the device bus* **[Gardner discloses in paragraphs [0134]-[0135], "SPK 36 provides abstractions to allocate, map, unmap, and free virtual addresses..."]."** **(See rejection of claim 7).**

With respect to **claims 9 and 18**,

"A data processing apparatus as claimed in claim 8 **[see rejection of claim 8]**, *wherein the chip further comprises: further memory coupled to the processor via a system bus, the further memory operable to store data required by the processor,* **[Gardner discloses in paragraph [0157], "If the number of active protection keys is greater than the available protection key registers 118, SPK 36 employs the protection key registers as a cache." Gardner teaches in FIG.3, a processor (element 32), a cache (element 118), and a further memory unit (element 20), which is coupled to the processor via a system bus (FIG.3) and is operable to store data required by the processor.**

Furthermore, Gardner discloses in paragraph [0003], "...The Intel Architecture (IA-64) and the HP Precision Architecture (PA-RISC) type processors..." It is notoriously well known that the Intel Architecture (IA-64) and the HP Precision Architecture (PA-RISC) comprises a device bus via which each device is connectable to a further memory unit.]"

"...the further memory comprising secure further memory for storing secure data and non-secure further memory for storing non-secure data; is disclosed in **paragraph [0026] as stated supra (also see rejections of claims 1 and 2).**

"...and further partition checking logic coupled to the system bus and operable whenever the memory access request is generated by the processor when operating in a non-secure mode in said non-secure domain to detect if the memory access request is seeking to access either the secure memory or the secure further memory, and upon such detection to prevent the access specified by that memory access request **[Gardner discloses in paragraph [0026], "Secure platform 40, however, ensures that one domain cannot accidentally or intentionally access another domain's memory." Gardner next discloses in paragraph [0195], "Using the memory management services of SPK 36, a user application is able to create secure memory partitions and processes to protect information in memory from all other applications and operating systems running on the system, even including the operating system under which it is running."]." (Also see rejection of claim 5)**

CONCLUSION

Status of Claims in the Application

The following is a summary of the treatment and status of all claims in the application as recommended by **M.P.E.P. 707.07(i):**

Claims rejected in the Application

Per the instant office action, claims **1-20** have received a first action on the merits and are subject of a first action non-final.

Direction of Future Correspondences

Any inquiry concerning this communication or earlier communication from the examiner should be directed to Horace L. Flournoy whose telephone number is (571) 272-2705. The examiner can normally be reached on Monday through Friday 8:00 AM to 5:30 PM (ET).

Important Note

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Don Sparks can be reached on (571) 272-4201. The fax phone numbers for the organization where this application or proceeding is assigned is (703) 746-7239.

Information regarding the status of an Application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or PUBLIC PAIR. Status information for unpublished applications is available through Private Pair only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

DONALD SPARKS
SUPERVISORY PATENT EXAMINER

Horace L. Flournoy

Patent Examiner

Art unit: 2189

Supervisory Patent Examiner

Technology Center 2100